



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,444	07/05/2001	Elsie Van Herreweghen	CH92000009US1	4090

7590 02/24/2005
IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/899,444	HERREWEGHEN, ELSIE VAN	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____ | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

1. Claims 1-35 have been examined.

Claim Objections

2. Claim 29 is not a complete sentence nor does the claim further define any features patentably distinct from known program storage devices as recited in the preamble of the claim.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1, 6, 13 and 24-26 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for a receipt including transaction relevant data composed by a transaction server, a pseudonym used by the initiator of the request taken from the transaction request message and the issuer of the receipt (see specification, pg. 13, 1st full paragraph, last sentence), does not reasonably provide enablement for a receipt that includes details for what the receipt has been given (or issued) and a reference to the owner (or designated owner) of the receipt. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make the invention commensurate in scope with

these claims. The recited claim language that defines the receipt as including details for what said receipt has been given (claims 1, 6, 24 and 25) or the receipt including information related to a purpose for which said receipt has been given (claims 13 and 26) appear to generalize to any information related to the context of the receipt. This recited limitation is broader than the enabling portion of the specification.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 15, 16, 21 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claim 15 recites the limitation "the second addressee". There is insufficient antecedent basis for this limitation in the claim. It is herein assumed claim 15 is dependent on claim 14.

8. Claim 16 recites the limitation "the second private signature". There is insufficient antecedent basis for this limitation in the claim. It is herein assumed claim 16 is dependent on claim 14.

9. Claim 21 recites the limitation "the first and second message". There is insufficient antecedent basis for this limitation in the claim. It is herein assumed claim 21 is dependent on claim 20.

10. Claim 22 recites the limitation "the first and second message". There is insufficient antecedent basis for this limitation in the claim. It is herein assumed claim 22 is dependent on claim 20.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 29 is rejected under 35 U.S.C. 101 because the claimed invention lacks patentable utility. The claim defines only a program storage device readable by machine and tangibly embodying a program of instructions executable by the machine to perform method steps.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

13. Claims 6, 7, 11, 13, 19, 20, 25-28, 31, 32, 34 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Lewis et al. U.S. Patent No. 6,233,565 (hereinafter Lewis).

14. As per claim 6, Lewis discloses a receipt generation method, comprising generating an electronic receipt in a communication system providing a public key encryption system, including the steps of:

- a. receiving a message from a sender, the message is electronically signed by the sender using a private signature key owned by the sender, whereby the message includes a transaction request and a reference to a designated owner of a receipt to be generated (see Lewis, col. 4:20-27);
- b. authenticating the message using a public signature verification key associated to the private signature key held by the sender of the message (see Lewis, 4:24-27; cols. 7 and 8: TABLE 1 under "Transaction Type": "authentication client 2n to server", under "Transaction Server 190" and "Master Server 300");
- c. issuing a receipt including the reference to the designated owner of the receipt and details for what the receipt has been given (see Lewis, 4:32-38); and

- d. electronically signing the receipt with a public signature key assigned to an issuer issuing the receipt (see Lewis, 4:41-44).

The aforementioned cover the limitations of claim 6.

15. As per claim 7, the rejection of claim 6 is incorporated herein. In addition, the method further includes the steps of performing the requested transaction, and returning the receipt to the sender. See Lewis, col. 4:32-33.

16. As per claim 11, the rejection of claim 6 is incorporated herein. In addition, the designated owner of the receipt is the sender. See Lewis, col. 4:32-35.

17. As per claim 13, the rejections of claims 7 and 11 are incorporated herein. In addition, the method disclosed by Lewis, is also a method of proving ownership of a receipt (holder of the digital receipt signed by both the owner and the issuer proves ownership of the receipt) including the steps of:

- e. creating a first message including a transaction request and a reference to a designated owner of a receipt to be generated in response to receiving the message (see Lewis, col. 4, 20-27; the sender of the transaction request is the designated owner of the receipt);
- f. electronically signing the message using a first private signature key (see Lewis, 4:24-25; cols. 7 and 8: TABLE 1 under "Transaction Type": "authentication client 2n to server");

- g. sending the first message to a first addressee (see Lewis, 4:20-27; first addressee is the transaction server; and
- h. receiving the receipt from the first addressee, the receipt being electronically signed by the first addressee having given the receipt using a private signature key assigned to the first addressee, wherein the receipt includes information as for what the receipt has been issued and the reference to the designated owner of the receipt (see Lewis, 4:32-43).

The aforementioned cover the limitations of claim 13.

18. As per claim 19, the rejection of claim 13 is incorporated herein. In addition, the designated owner of the receipt is identical to a sender sending the first message to the first addressee. See Lewis, col. 4, 20-27; the sender of the transaction request is the designated owner of the receipt.

19. As per claim 20, the rejections of claims 13 and 19 are incorporated herein. In addition, the method further comprises creating a second message including the receipt; electronically signing the second message using a second private signature key; and sending the second message to the designated owner of the receipt. See Lewis, col. 4:32-43.

20. As per claims 25 and 26, they are apparatus claims corresponding to claims 6 and 13, and they do not teach or define above the information claimed in claims 6 and

13. Therefore, claims 25 and 26 are rejected as being anticipated by Lewis for the same reasons set forth in the rejections of claims 6 and 13.

21. As per claims 27, 28, 31 and 32, the rejections of claims 6 and 13 are incorporated herein. In addition, means to perform the methods of claims 6 and 13 are embodied in a program of instructions executable by a machine. See Lewis, Figure 2.

22. As per claims 34 and 35, the rejections of claims 6, 13, 25, 26, 27, 28, 31 and 32, are incorporated herein. In addition, means to effect the functions of the devices of claims 25 and 26 comprise computer readable program. See Lewis, col. 2:10-14.

Claim Rejections - 35 USC § 103

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

24. Claims 8-10 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Brands U.S. Patent No. 5,604,805 (hereinafter Brands).

25. As per claims 8-10, the rejection of claim 6 is incorporated herein. Lewis does not teach using a pseudonym for communicating nor using a pseudonym as a reference to a designated owner. Brands discloses using pseudonyms to withhold the identity of a

user in transactions requiring certifying signatures, wherein the signature remains anonymous. See Brands, col. 2:15-34. It would be obvious to one of ordinary skill in the art at the time the invention was made to use a pseudonym for communication and designating the owner with a pseudonym to be used as a reference to the owner.

Motivation to combine guarantees the privacy of a user transferring certified information. See Brands, col. 2:15-16. Finally, an anonymous communication connection is necessarily required in a pseudonym protocol. The aforementioned cover the limitations of claims 8-10.

26. As per claim 17, the rejections of claims 8-10 and 13 are incorporated herein. In addition, the reference to the designated owner of the receipt is a pseudonym used by the owner of the receipt. It would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to the designated owner of the receipt to be a pseudonym used by the owner of the receipt. Motivation to combine guarantees the privacy of a user transferring certified information. See Brands, col. 2:15-16.

27. Claims 1, 2, 5, 12, 14, 16, 18, 23, 24, 30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Muftic U.S. Patent No. 5,850,442 (hereinafter Muftic).

28. As per claim 1, Lewis discloses a method comprising generating an electronic receipt in a communication system providing a public key encryption infrastructure,

Art Unit: 2132

wherein a server generation module in response to an electronic payment transaction, generates a receipt and transmits the receipt, wherein the receipt comprises a client digital signature and a the server digital signature, and a data set uniquely identifying the executed transaction, and further wherein the receipt authenticates the electronic transaction. See Muftic, col. 4:24-44.

29. Lewis does not expressly teach how the electronic receipt is authenticated.

Muftic teaches an ordinary means of authenticating a signed message by a sender of the message using a public key encryption infrastructure including the following steps:

- i. receiving a message from a sender, the message being electronically signed by the sender using a private signature key owned by the sender; the corresponding public key of the sender is provided within a digital certificate by a trusted issuer and signed by the issuer having given the certificate, wherein the certificate includes details for the context of the certificate and a reference to the owner of the certificate (see Muftic, col. 2:42-51; 3:35-52; 4:27-32; digital certificates in the standard X.509 define attributes including certificate context and key subscriber identity values);
- j. obtaining a public signature verification key on the basis of the reference to the owner of the certificate (digital certificates enables trusted retrieval of the public signature verification key); and
- k. examining whether or not the private signature key used for electronically signing the message is associated to the public signature verification key

obtained on the basis of the reference to the owner of the certificate (see Muftic, 2:44-51).

30. Although Muftic does not expressly teach submitting the certificate holding the public signature verification key and signed by the issuer with the original signed message; including the certificate with the signed message is a trivial combination since adequate verification of the signed message requires the signed certificate (see Muftic, 3:30-33); moreover, the combination of disparate parts has been found to be an obvious feature. See *In re Larson* 144 USPQ 347 (CCPA 1965). Further, the digital certificate taught by Muftic is operatively equivalent to the electronic receipt: both maintain a record of an agreement/transaction between the owner and the issuer. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made given the invention of Lewis wherein the receipt is signed by both the owner of the receipt and the issuer of the receipt, and the verification steps taught by Muftic, to verify the receipt according to the recited steps of applicant's claim 1. Motivation to combine verifies the receipt as being owned by the sender and issued by the issuer. See Lewis, 4:36-38; Muftic, 2:10-14 and 3:47-49. The aforementioned cover the limitations of claim 1.

31. As per claim 2, the rejection of claim 1 is incorporated herein. In addition, the reference to the owner of the receipt is a public signature verification key associated to a private signature key held by the owner of the receipt. See Muftic, col. 2:15-25.

32. As per claim 5, the rejection of claim 1 is incorporated herein. In addition, the method further comprises the step of authenticating the receipt using a public signature verification key assigned to the issuer of the receipt. See Muftic, col. 3:51-52.

33. As per claim 12, the rejection of claims 1 and 6 is incorporated herein. In addition, the reference to a designated owner is a public signature key associated to a private signature verification key held by the designated owner of the receipt. See Muftic, col. 3:35-41. It would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to a designated owner to be a public signature key associated to a private signature verification key held by the designated owner of the receipt. Motivation to combine enables public key verification of a signature signed with the owner's private key using a certified public key. See Muftic, 2:6-14 and 3:35-52. The aforementioned cover the limitations of claim 12.

34. Regarding claims 14 and 16, the rejection of claims 1 and 13 are incorporated herein. In addition, as argued in the rejection of claim 1, verification of the receipt signed by both the sender and the issuer is an obvious step. Further, a mediating service distinct from the owner of the receipt necessarily verifies the ownership of a receipt. Finally, Muftic teaches verifying a signed message by decrypting the signed message and comparing the decrypted message with an original message for equality (see Muftic, col. 2:41-51), which is functionally obvious over the step of comparing two electronic signatures for equality as recited in claim 16.

35. Regarding claim 18, the rejections of claims 12 and 13 are incorporated herein. In addition, the reference to a designated owner is a public signature key associated to a private signature verification key held by the designated owner of the receipt. See Muftic, col. 3:35-41. It would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to a designated owner to be a public signature key associated to a private signature verification key held by the designated owner of the receipt. Motivation to combine enables public key verification of a signature signed with the owner's private key using a certified public key. See Muftic, 2:6-14 and 3:35-52. The aforementioned cover the limitations of claim 18.

36. As per claim 24, it is an apparatus claims corresponding to claim 1, and it does not teach or define above the information claimed in claim 1. Therefore, claim 24 is rejected as being unpatentable over Lewis in view of Muftic for the same reasons set forth in the rejection of claim 1.

37. As per claims 23 and 30, the rejections of claims 1 and 24 are incorporated herein. In addition, means to perform the method of claim 1 is embodied in a program of instructions executable by a machine. See Lewis, Figure 2.

38. As per claim 33, the rejections of claims 1, 23, 24 and 30, are incorporated herein. In addition, means to effect the functions of the device of claim 24 comprise a computer readable program. See Lewis, col. 2:10-14.

39. Claims 3, 4, 15, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Muftic and Brands.

40. As per claims 3 and 4, the rejection of claims 2 and 8-10 are incorporated herein. In addition, the reference to the owner of the receipt is a pseudonym used by the owner of the receipt and a certificate securely links the pseudonym to the public signature verification key. See Brands, col. 2:15-34 (blind signature protocol links the pseudonym with the user); see Muftic, col. 2:15-25. It would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to the owner of the receipt to be a pseudonym used by the owner of the receipt and for a certificate to securely link the pseudonym to the public signature verification key. Motivation to combine guarantees the privacy of a user transferring certified information. See Brands, col. 2:15-16. The aforementioned cover the limitations of claims 3 and 4.

41. As per claim 15, the rejection of claim 14 is incorporated herein. Lewis does not expressly teach the first addressee is identical to the second addressee. However, Brand teaches it is well known for participants involved in electronic protocols consisting of roles, including: users, certifying parties and transaction parties, to perform more than

one of these roles. See Brands, col. 1:17-25. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first addressee to be identical to the second addressee since consolidation of roles enables participants to be more flexible in the roles they perform as taught by Brands, *ibid.* Furthermore, it is desirable for a server issuing a receipt to be able to validate the receipt, since a receipt acts as a record of services requested and paid for by the user.

42. As per claims 21 and 22, the rejections of claims 8-10 and 20 are incorporated herein. Further, Lewis discloses using pseudonyms to withhold the identity of a user in transactions requiring the use of certifying a signature, wherein the signature remains anonymous. See Brands, col. 2:15-34. It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the sending and receiving of the first and second messages are performed by using a pseudonym. Motivation to combine guarantees the privacy of a user transferring certified information. See Brands, col. 2:15-16. Finally, an anonymous communication connection is necessarily required in a pseudonym protocol. The aforementioned cover the limitations of claims 21 and 22.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hippelainen U.S. Patent No. 6,516,996 discloses using electronic receipts to collect financial transaction data.

Makipaa et al. U.S. Patent No. 6,394,341 discloses generating, transferring and validating receipts using public key encryption.

Chaum "Security without identification: Transaction Systems to Make Big Brother Obsolete".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

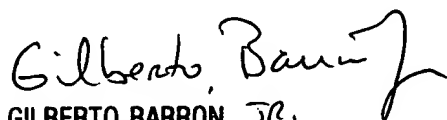
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
February 15, 2005



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100